

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 1月19日

出 願 番 号

Application Number:

特願2001-011248

出 願 人

Applicant(s):

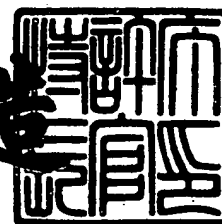
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月30日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3105305

【書類名】 特許願

【整理番号】 2037320014

【提出日】 平成13年 1月19日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 3/14

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 秦 秀彦

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 稲見 聡

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 和田 浩美

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 水山 正重

【発明者】

【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 松下通信工業株式会社内

【氏名】 加藤 淳展

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 情報端末装置

【特許請求の範囲】

【請求項 1】サーバ装置から取得した指示データによって端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの妥当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末用データを格納する端末内データ格納手段とを備え、前記動作制御手段により前記送受信手段へ前記端末用データを取得する指示を行い、取得した前記端末用データを前記動作制御手段によって、前記端末内データ格納手段へ反映することを特徴とする情報端末装置。

【請求項 2】前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記サーバ装置より取得した前記端末用データを端末の表示画面に表示させることを特徴とする請求項 1 記載の情報端末装置。

【請求項 3】前記解析手段は、前記妥当性判定手段の結果をもとに、解析を行うことを特徴とする請求項 1 記載の情報端末装置。

【請求項 4】前記端末用データは、端末を制御するためのデータであり、端末内データ格納手段に端末用データを反映させることにより、端末の制御を行うことを特徴とする請求項 1 記載の情報端末装置。

【請求項 5】前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする請求項 1 記載の情報端末装置。

【請求項 6】前記動作制御手段は、J A V A V M 上で動作する J A V A アプレットによって構成され、前記 J A V A アプレットはインターネット上のサーバ装置より取得することを可能とすることを特徴とする請求項 1 記載の情報端末装

置。

【請求項 7】前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする請求項 1 記載の情報端末装置。

【請求項 8】前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする請求項 1 記載の情報端末装置。

【請求項 9】サーバ装置から取得した指示データによって端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの妥当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末内データを格納する端末内データ格納手段とを備え、前記解析手段の結果を、前記動作制御手段によって、端末の制御を行う前記端末内データ格納手段に反映させることを特徴とする情報端末装置。

【請求項 10】前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記動作制御手段が反映させた前記端末内データ格納手段のデータを端末の表示画面に表示させることを特徴とする請求項 9 記載の情報端末装置。

【請求項 11】前記解析手段は、前記妥当性判定手段の結果をもとに、解析を行うことを特徴とする請求項 9 記載の情報端末装置。

【請求項 12】前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする請求項 9 記載の情報端末装置。

【請求項 13】前記動作制御手段は、J A V A V M 上で動作する J A V A アプレットによって構成され、前記 J A V A アプレットはインターネット上のサー

バ装置より取得することを可能とすることを特徴とする請求項 9 記載の情報端末装置。

【請求項 1 4】前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする請求項 9 記載の情報端末装置。

【請求項 1 5】前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする請求項 9 記載の情報端末装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報端末装置に関し、特に指示データの妥当性を判定する方式を用いることによって、周辺機器への制御を安全に行える情報端末装置に関する。

【0 0 0 2】

【従来の技術】

J A V A のプログラム形態の一つである J A V A アプレットにおいては、ネットワーク上で利用されることを目的としており、I n t e r n e t E x p l o r e r や N e t s c a p e C o m m u n i c a t o r と 言 っ た W E B ブラウザよりネットワーク側からダウンロードして実行することを可能にしている。しかし、安全面のことを考えそのようにして取得した J A V A アプレットには、周辺機器のアクセスや I / O ポートへの読み書きと言った実行に制限がかかっている。そのため、J A V A アプレットが端末の中にあるデータの読み書きや I / O ポートへの読み書きと言った動作を行うことができなかった。

また、従来技術では、周辺機器への読み書きを行うために、J A V A アプレットが使用するライブラリに周辺機器のドライバを組み込むことによって、解決していた（特開 2 0 0 0 - 1 1 2 8 6 4）。

【0 0 0 3】

【発明が解決しようとする課題】

しかしながら、上述のように、携帯電話や携帯情報端末など、自由に J A V A VMに含まれる J A V A ライブラリを、追加できない装置にあとからライブラリを追加することは不可能である。

【 0 0 0 4 】

このような装置にライブラリを追加するためには、あらかじめ、商品出荷時にこのようなライブラリを組み込んでおく必要がある。しかし、このようにしてしまうと、全てのユーザが周辺機器へアクセスできるライブラリを使用できてしまうことになってしまう。

【 0 0 0 5 】

また、携帯電話といった端末に関しては、利用者個人の特別な情報（電話番号、住所録など）が格納されている。このような情報を特権のないユーザが引き出してしまうことは問題である。

【 0 0 0 6 】

本発明は、上記従来技術の問題を解決し、周辺機器へアクセスするプログラムには、特権を持たせることによって、安全に周辺機器へのアクセスを行えることを特徴とする情報端末装置を提供することを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】

上記課題を解決するために、サーバ装置から取得した指示データによって端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの妥当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末用データを格納する端末内データ格納手段とを備え、前記動作制御手段により前記送受信手段へ前記端末用データを取得する指示を行い、取得した前記端末用データを前記動作制御手段によって、前記端末内データ格納手段へ反映することを特徴とする。

【 0 0 0 8 】

更に、前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記サーバ装置より取得した前記端末用データを端末の表示画面に表示させることを特徴とする。

【 0 0 0 9 】

また、前記解析手段と、前記妥当性判定手段は、前記妥当性判定手段の結果をもとに、前記解析手段を行うことを特徴とする。

【 0 0 1 0 】

また、前記端末用データは、端末を制御するためのデータであり、端末内データ格納手段に端末用データを反映させることにより、端末の制御を行うことを特徴とする。

【 0 0 1 1 】

また、前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする。

【 0 0 1 2 】

また、前記動作制御手段は、J A V A V M上で動作するJ A V Aアプレットによって構成され、前記J A V Aアプレットはインターネット上のサーバ装置より取得することを可能とすることを特徴とする。

【 0 0 1 3 】

また、前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする。

【 0 0 1 4 】

また、前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする。

【 0 0 1 5 】

更に、上記課題を解決するために、サーバ装置から取得した指示データによっ

て端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末内データを格納する端末内データ格納手段とを備え、前記解析手段の結果を、前記動作制御手段によって、端末の制御を行う前記端末内データ格納手段に反映させることを特徴とする。

【 0 0 1 6 】

更に、前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記動作制御手段が反映させた前記端末内データ格納手段のデータを端末の表示画面に表示させることを特徴とする。

【 0 0 1 7 】

また、前記解析手段と、前記妥当性判定手段は、前記妥当性判定手段の結果をもとに、前記解析手段を行うことを特徴とする。

【 0 0 1 8 】

また、前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする。

【 0 0 1 9 】

また、前記動作制御手段は、J A V A V M上で動作するJ A V Aアプレットによって構成され、前記J A V Aアプレットはインターネット上のサーバ装置より取得することを可能とすることを特徴とする。

【 0 0 2 0 】

また、前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする。

【 0 0 2 1 】

また、前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする。

【 0 0 2 2 】

【発明の実施の形態】

以下、本発明の実施例を図面を用いて詳細に説明する。

【 0 0 2 3 】

(実施の形態 1)

図 1 は、本発明の実施の形態 1 の情報端末装置を示すブロック図である。図 1 において、サーバ装置 1 0 1 は、インターネット上に存在し、HTML、画像データを保持し、要求に応じて、これらのデータを要求元へ送出する装置である。指示データ 1 0 2 は、サーバ装置 1 0 1 上に存在し、情報端末装置 1 0 4 への指示が記述されている。また、端末用データ 1 0 3 は、指示データ 1 0 2 によって、情報端末装置 1 0 4 が取得する端末用のデータである。情報端末装置 1 0 4 は、インターネット上のデータを取得し、表示することができる装置である。データ取得要求手段 1 0 5 は、指示データ 1 0 2 を取得するための手段である。送受信手段 1 0 6 は、データ取得要求手段 1 0 5 より要求のあった URL のデータを取得するための手段である。受信データ格納手段 1 0 7 は、送受信手段によって取得したデータを格納する手段である。解析手段 1 0 8 は、受信データ格納手段 1 0 7 に格納されている指示データを解析するための手段である。解析結果格納手段 1 0 9 は、解析手段 1 0 8 によって解析したデータを格納するための手段である。妥当性判定手段 1 1 0 は、解析結果格納手段 1 0 9 に格納されているデータより、指示データ 1 0 2 が妥当なデータであることを判定するための手段である。動作制御手段 1 1 1 は、妥当性判定手段 1 1 0 によって、指示データ 1 0 2 が妥当であると判定された際に、指示データ 1 0 2 に基づいて動作を行う手段である。端末内データ格納手段 1 1 2 は、動作制御手段 1 1 1 から送受信手段 1 0 6 へ取得要求を出し、その結果取得し、受信データ格納手段 1 0 7 に格納した端末用データ 1 0 3 を格納する手段である。表示手段 1 1 3 は、端末内データ格納手段 1 1 2 によって格納されている端末用データを用いて、表示を行うための手

段である。データ出力手段 1 1 4 は、動作制御手段 1 1 1 によって、指示されたデータを出力するための手段である。

【 0 0 2 4 】

上記のように構成された実施の形態 1 の情報端末装置の動作について、図 2 のフローチャートを用いて説明する。データ取得処理（ステップ 2 0 1）では、情報端末装置 1 0 4 は、WEB ブラウザに表示している画面からアンカーを選択するなどして、指示データ 1 0 2 を取得要求を行う処理を行う。送受信処理（ステップ 2 0 2）では、データ取得処理（ステップ 2 0 1）より取得要求のあった指示データ 1 0 2 を取得する処理を行う。解析処理（ステップ 2 0 3）では、取得した指示データ 1 0 2 の解析を行う。妥当性判定処理（ステップ 2 0 4）では、解析処理（ステップ 2 0 3）の結果をもとに取得した指示データ 1 0 2 が妥当なデータであるかどうかを判定する。動作制御処理（ステップ 2 0 5）では、指示データに記述された内容に従って端末用データ 1 0 3 を取得する処理を行う。送受信処理（ステップ 2 0 6）では、指示データに端末用データを取得する内容が記述されている際は、データの取得を行う。複数の端末用データの取得が記述されている際は、複数回データの取得を行う。表示処理（ステップ 2 0 7）では、動作制御処理（ステップ 2 0 5）と送受信処理（ステップ 2 0 6）によって取得した端末用データの表示を行う。

【 0 0 2 5 】

ステップ 2 0 2 において送受信手段 1 0 6 によってサーバ装置 1 0 1 から取得できるデータについて図 6、図 8 を用いて説明する。サーバ装置 1 0 1 より取得する指示データは、図 6 のように XML (Extended Markup Language) 形式のフォーマットを持つ。なお、このフォーマットは「タグ名：値」と言った形式でもよく、このフォーマットのみに限らない。protected タグ 6 0 1 と dataSourceUrl タグ 6 0 2 と signature タグ 6 0 4、certificate タグ 6 0 5 が妥当性の判定に用いられる部分である。protected タグ 6 0 1 の部分に端末装置 1 0 4 に対する指示内容が記述される。端末用データ 1 0 3 として取得されるデータが、図 8 である。dataSourceUrl タグ 6 0 2 の部分に記述されている内容がに

わとりの画像データ801、パンダの画像データ802と言ったデータである。なお、このデータは画像データのみではなく、音楽データや制御用データであっても構わない。また、exDataDigestタグ603は、ステップ205で端末用データ103の妥当性の判定に用いられる。指示データ102は、ステップ203で受信した際は、DESアルゴリズムによって暗号化が行われている。なお、この暗号化に用いられる方式は、DESアルゴリズムに関わらず、様々な暗号化方式で暗号化される。

【0026】

次にステップ203について図3を用いて説明する。暗号復号処理（ステップ302）では、指示データ102が暗号化されている際は、暗号化されている指示データ102の復号化を行う。また、復号化のアルゴリズムには、DESなどの様々なアルゴリズムが用いられる。なお、指示データ102は、必ずしも復号されているとは限らない。指示データ解析処理（ステップ303）では、復号化が終了した指示データの解析を行う。解析の結果は、解析結果格納手段109に格納される。

【0027】

図7はステップ203によって、解析された結果が解析結果格納手段109に格納される一例を示している。解析に用いた指示データの種別を識別するための情報(descriptorType)には、Customiseが格納されている。指示データのバージョンを示す情報(FID)には、1が格納されている。指示データを受けて動作制御部が取得しに行く必要がある端末用データ103が格納されている場所(dataSourceUrl)には、https://www.hoge.com/fool.gifとhttps://www.hoge.com/fool2.gifが格納されている。dataSourceUrlが示す端末用データを、MD5アルゴリズムを用いてハッシュ化した情報(exDataDigit)にはそれぞれに対応してafdfsafafafkljk:jbahaf1kdjfaとbhoybyouhsdholidioubが格納されている。署名の情報(signature)には署名が格納されている。署名者の証明書を格納する情報(certificate)には、その

値である署名者の証明書と二次CAの証明書が格納される。なお、場合によっては、二次CA証明書は存在しない場合もあり、更に三次、四次と続く場合もある。

【0028】

次にステップ204について図4と図6を用いて説明する。指示データ606の<protected>タグと</protected>タグ囲まれるデータについてMD5 (Message Digest 5) アルゴリズムでハッシュ化を行う (ステップ402)。なお、ハッシュ化を行うためのアルゴリズムは、MD5だけに限らない。なお、ハッシュ化を行う指示データの範囲は、指示データ606に限るものではなく、取り決めることができる。N次証明書の妥当性判定処理 (ステップ403) と署名者の証明書の判定処理 (ステップ404) では、certificateタグ605の署名者の証明書が妥当であると証明できるまで、順に証明書、二次証明書と利用し、場合によっては、N次証明書を利用して妥当性の判定を行う。なお、証明書はインターネットの世界で一般的に用いられている公開鍵暗号方式に用いられる証明書である。公開鍵取得処理 (ステップ405) では、署名者の証明書より公開鍵の取得を行う。署名復号化処理 (ステップ406) では、署名部分604を公開鍵取得処理で取得した公開鍵を用いることによって復号を行う。ハッシュ化データ比較処理 (ステップ407) では、ステップ402で取得したハッシュ値とステップ406で取得した署名の値を比較する。比較結果が正しければ指示データ606は妥当だと証明されたデータと考えられる。なお、ステップ403に、用いられる妥当性を判定する処理には、公開鍵暗号方式だけに限らない。

【0029】

次に図5を用いてステップ205の説明をする。まず解析結果格納手段109を参照し、データ取得判定処理 (ステップ502) を行う。解析結果格納手段109に取得すべき端末内データが存在するだけデータ取得処理 (ステップ503) に取得を行う。データ妥当性判定処理 (ステップ504) では、取得した端末用データ103が妥当であるか否かの判定を行う。妥当性の判定は、取得したデータをMD5アルゴリズムでハッシュ化し、その値が解析結果格納手段109に

格納されているMD5の値と比較し、等しければ妥当だと判定する。なお、ステップ504はなくても構わない。なお、ステップ504に用いるアルゴリズムはMD5アルゴリズムに限らない。端末内データ格納処理（ステップ505）では、妥当性を判定できた端末用データ103を端末内のデータとして格納する。なお、ステップ205は、J A V A アプレットのように動的に端末にダウンロードされるプログラムであっても構わない。なお、指示データに内容によって取得した端末用データを端末内データ格納手段112に格納するのではなく、データ出力手段（周辺機器、I r D A など）に出力することも考えられる。

【0030】

図2に示されるステップを行った結果、表示処理（ステップ207）で表示される様子を図9に示す。本発明によって表示が変更される前の様子901が、本発明によって表示が変更された後の様子902になる。本発明によって、端末内のデータの変更を安全に行い、表示する様子を変更することができた。

【0031】

（実施の形態2）

図1は、本発明の実施の形態2の情報端末装置を示すブロック図であり、実施の形態1の構成と同じである。情報端末装置の動作について、図10のシーケンス図を用いて説明する。データ取得処理（ステップ201）では、情報端末装置104は、WEBブラウザに表示している画面からアンカーを選択するなどして、指示データ102を取得要求を行う処理を行う。送受信処理（ステップ202）では、データ取得処理（ステップ201）より取得要求のあった指示データ102を取得する処理を行う。解析処理（ステップ203）では、取得した指示データ102の解析を行う。妥当性判定処理（ステップ204）では、解析処理（ステップ203）の結果をもとに取得した指示データ102が妥当なデータであるかどうかを判定する。動作制御処理（ステップ1005）では、指示データに記述された内容に従って端末内のデータを変更する処理を行う。複数の端末用データの変更が記述されている際は、複数回データの変更を行う。端末内データ格納処理（ステップ1006）では、動作制御処理（ステップ1005）によって指定されたデータの変更を行う。

【0032】

ステップ202によってサーバ装置101から取得できるデータについて図11を用いて説明する。サーバ装置より取得する指示データは、図11のようにXML (Extended Markup Language) 形式のフォーマットを持つ。なお、このフォーマットは「タグ名: 値」と言った形式でもよく、このフォーマットのみに限らない。protectedタグ1101とsignatureタグ1103、certificateタグ1104が妥当性の判定に用いられる部分である。protectedタグ1101の部分に端末装置104に対する指示内容が記述される。指示データ102は、ステップ203で受信した際は、DESアルゴリズムによって暗号化が行われている。なお、この暗号化に用いられる方式は、DESアルゴリズムに関わらず、様々な暗号化方式で暗号化される。

【0033】

ステップ203については実施の形態1と同様であるので省略する。

【0034】

図12はステップ203によって、解析された結果が解析結果格納手段109に格納される一例を示している。解析に用いた指示データの種別を識別するための情報(descriptorType)には、Controlが格納されている。指示データのバージョンを示す情報(FID)には、1が格納されている。指示データを受けて動作制御部がデータを反映する情報が格納されている場所(ctrlData)には、123が格納されている。署名の情報(signature)には署名が格納されている。証明書を格納する情報(certificate)には、その値である署名者の証明書と二次CAの証明書が格納されている。なお、場合によっては、二次CA証明書は存在しない場合もあり、更に三次、四次と続く場合もある。

【0035】

次にステップ204について図4と図11を用いて説明する。指示データ1105の<protected>タグと</protected>タグ囲まれるデータについてMD5 (Message Digest 5) アルゴリズムでハッ

シュ化を行う（ステップ402）。なお、ハッシュ化を行うためのアルゴリズムは、MD5だけに限らない。なお、ハッシュ化を行う指示データの範囲は、指示データ1101の部分に限るものではなく、取り決めることができる。N次証明書の妥当性判定処理（ステップ403）と署名者の証明書の判定処理（ステップ404）では、certificateタグ1104の署名者の証明書が妥当であると証明できるまで、順に証明書、二次証明書と利用し、場合によっては、N次証明書を利用して妥当性の判定を行う。なお、証明書はインターネットの世界で一般的に用いられている公開鍵暗号方式に用いられる証明書である。公開鍵取得処理（ステップ405）では、署名者の証明書より公開鍵の取得を行う。署名復号化処理（ステップ406）では、署名部分1103を公開鍵取得処理で取得した公開鍵を用いることによって復号を行う。ハッシュ化データ比較処理（ステップ407）では、ステップ402で取得したハッシュ値と署名復号化処理（ステップ406）で取得した署名の値を比較する。比較結果が正しければ指示データ1105は妥当性だと証明されたデータと考えられる。なお、妥当性判定処理に、用いられる妥当性を判定する処理には、公開鍵暗号方式だけに限らない。

【0036】

次に図13を用いてステップ1005の説明をする。まず解析結果格納手段109を参照し、データ取得判定処理（ステップ1302）を行う。解析結果格納手段109に取得すべき端末内データが存在するだけデータ取得処理（ステップ1303）にて取得を行う。端末内データ格納処理（ステップ1305）では、指示データに記述されたデータを端末内のデータとして端末内データ格納手段112に格納する。なお、ステップ1305は、JAVAアプレットのように動的に端末にダウンロードされるプログラムであっても構わない。なお、指示データに記述された内容を端末内データ格納手段112に格納するのではなく、データ出力手段114（周辺機器、IrDAなど）に出力することも考えられる。

【0037】

図10に示されるステップを行った結果、端末内のデータを変更することができた。

【0038】

【発明の効果】

JAVAアプレットのみに限らず、周辺機器へアクセスするプログラムにおいて、指示データに自身の妥当性を判定する方式を用いることによって、周辺機器の制御を安全に行える。

【図面の簡単な説明】

【図 1】

本発明の実施の形態の情報端末装置の示す全体構成図

【図 2】

本発明の実施の形態 1 の情報端末装置の動作を示すフローチャート

【図 3】

本発明の実施の形態 1 の解析処理を示すフローチャート

【図 4】

本発明の実施の形態 1 の妥当性判定処理を示すフローチャート

【図 5】

本発明の実施の形態 1 の動作制御処理を示すのフローチャート

【図 6】

本発明の実施の形態 1 の指示データの一例を示す図

【図 7】

本発明の実施の形態 1 の指示データの解析結果の一例を示す図

【図 8】

本発明の実施の形態 1 の端末用データの一例を示す図

【図 9】

本発明の実施の形態 1 の動作結果の一例を示す図

【図 10】

本発明の実施の形態 2 の情報端末装置の動作を示すフローチャート

【図 11】

本発明の実施の形態 2 の指示データの一例を示す図

【図 12】

本発明の実施の形態 2 の指示データの解析結果の一例を示す図

【図 1 3】

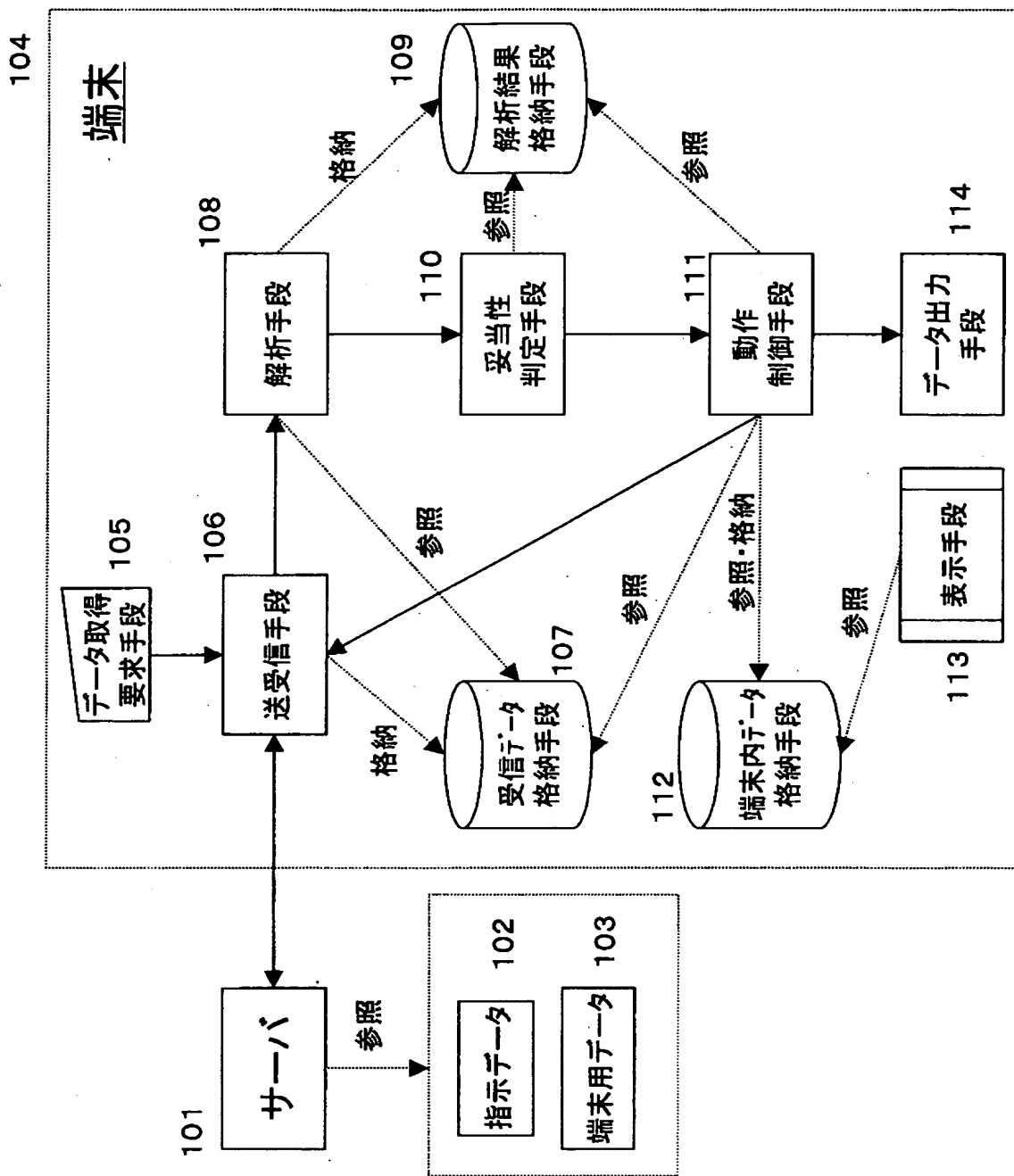
本発明の実施の形態 2 の動作制御処理を示すフローチャート

【符号の説明】

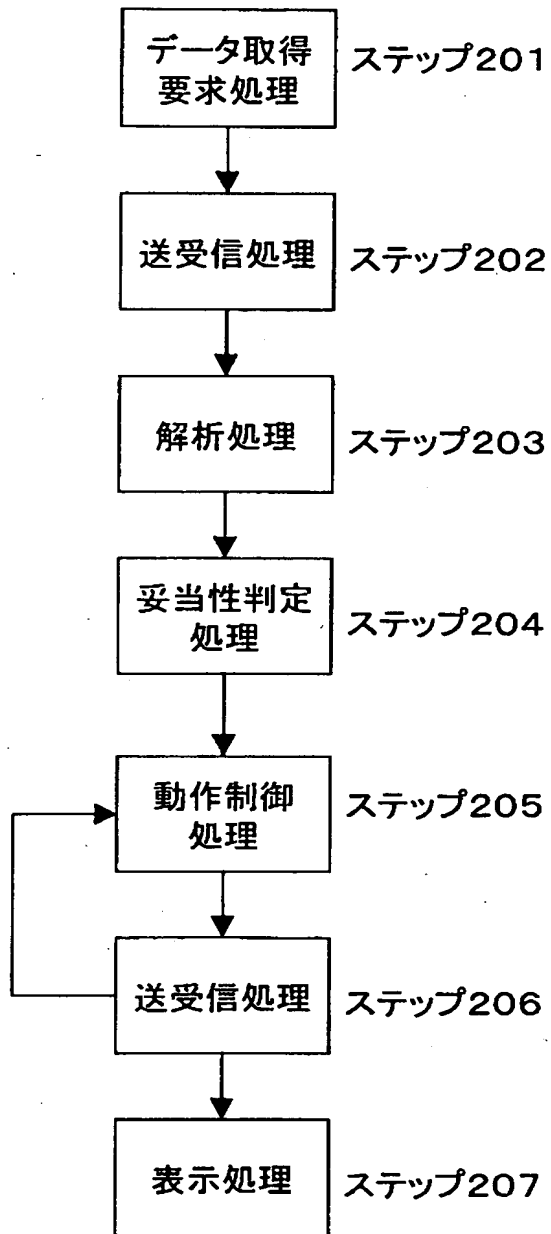
- 1 0 1 サーバ装置
- 1 0 2 指示データ
- 1 0 3 端末用データ
- 1 0 4 情報端末装置
- 1 0 5 データ取得要求手段
- 1 0 6 送受信手段
- 1 0 7 受信データ格納手段
- 1 0 8 解析手段
- 1 0 9 解析結果格納手段
- 1 1 0 妥当性判定手段
- 1 1 1 動作制御手段
- 1 1 2 端末内データ格納手段
- 1 1 3 表示手段
- 1 1 4 データ出力手段

【書類名】 図面

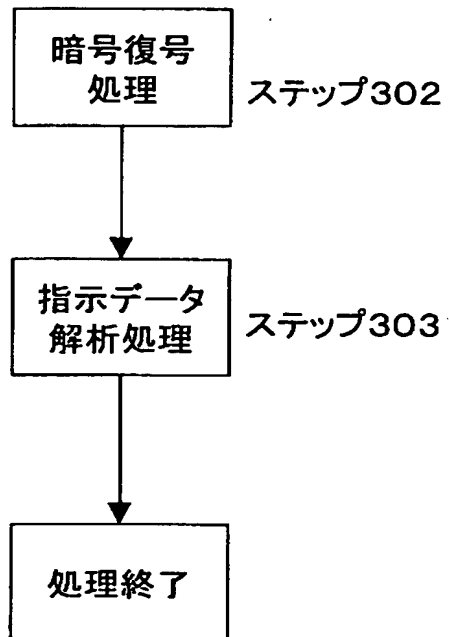
【図 1】



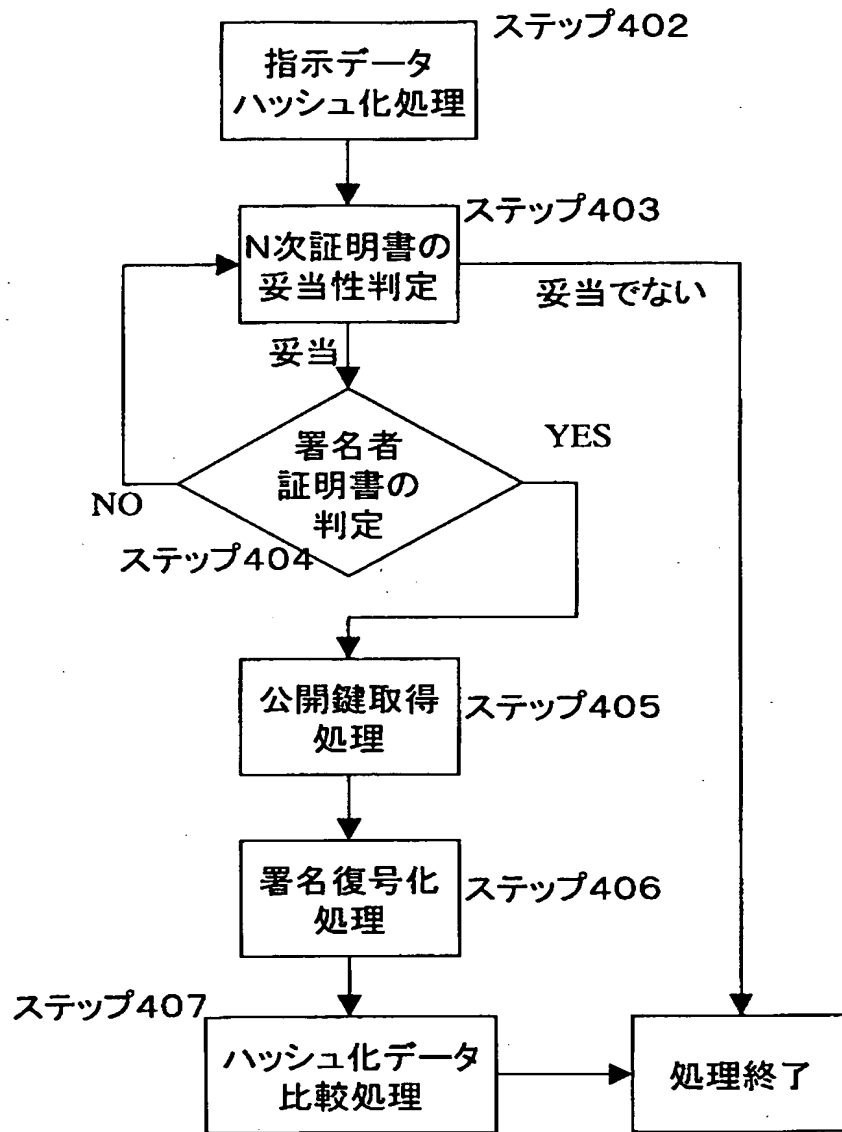
【図 2】



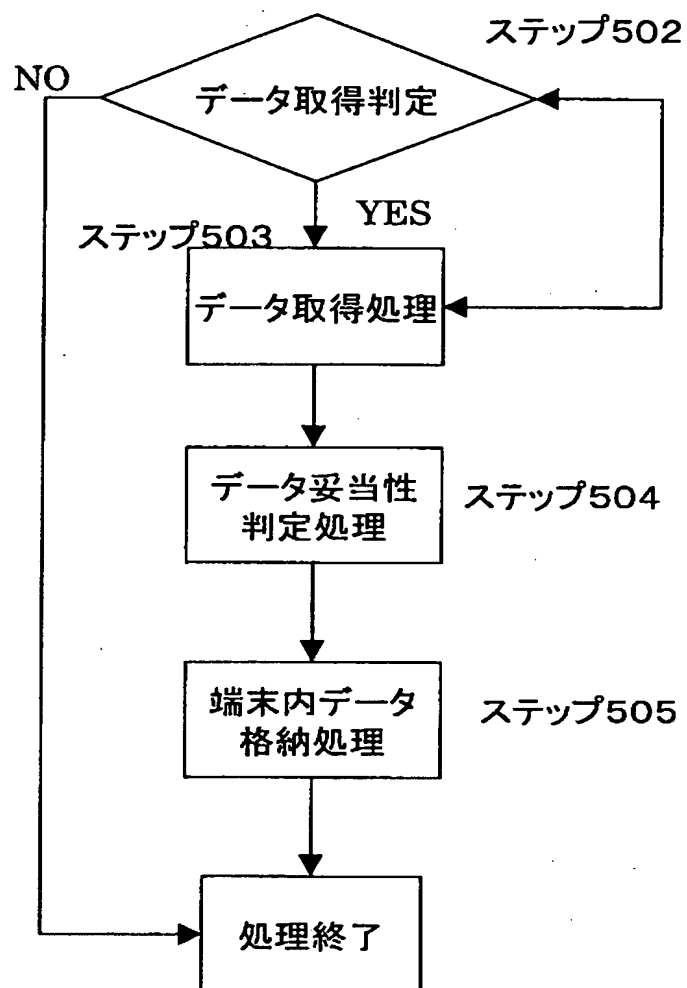
【図 3】



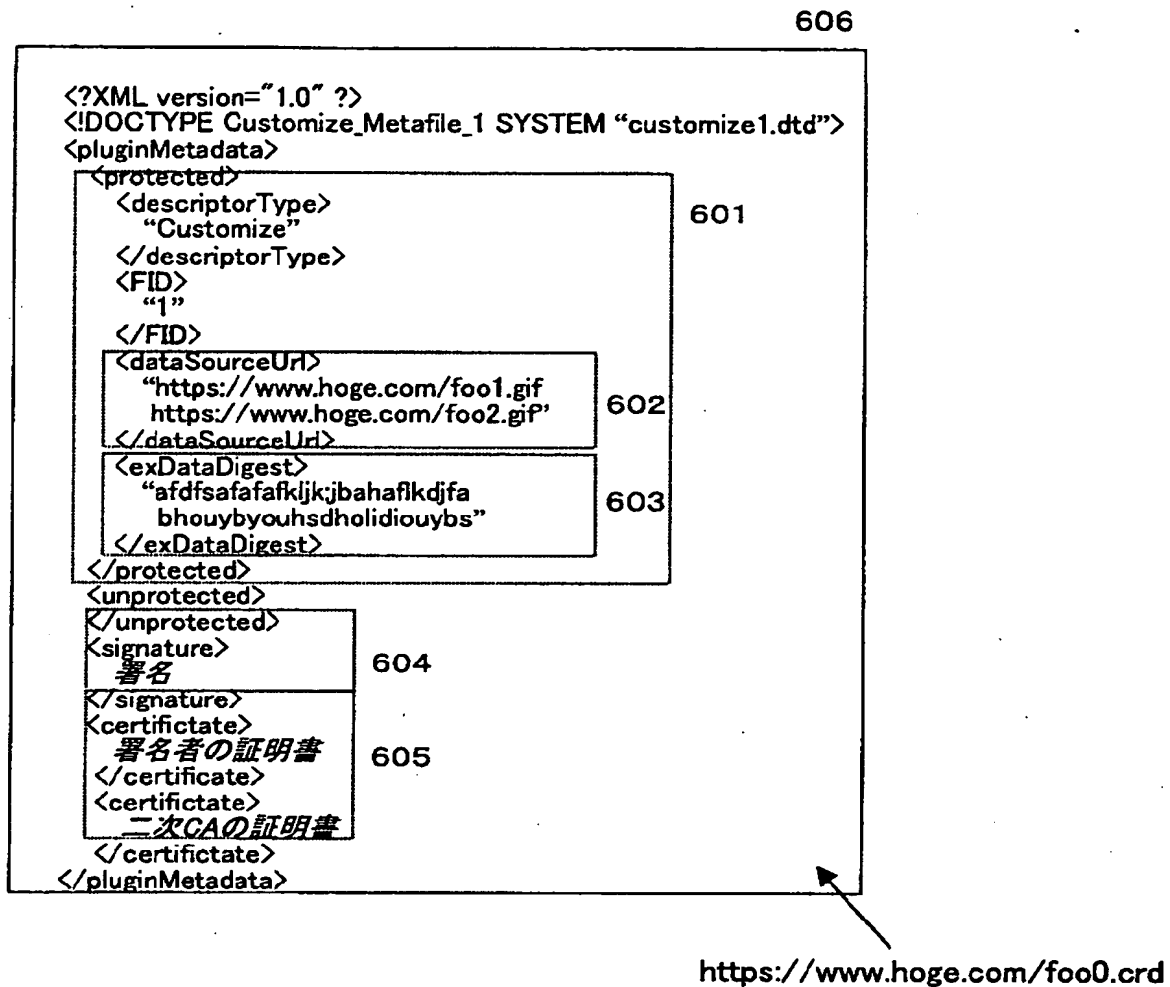
【図 4】



【図 5】



【図 6】



【図 7】

descriptorType	Customize
FID	1
dataSourceUrl	https://www.hoge.com/foo1.gif
dataSourceUrl	https://www.hoge.com/foo2.gif
exDataDigest	afdfsafafafkljkjbahafldjfa
exDataDigest	bhouybyouhsdholidiouybs
signature	署名
certificate	署名者の証明書
certificate	二次CAの証明書

【図 8】



<https://www.hoge.com/foo1.gif>

801

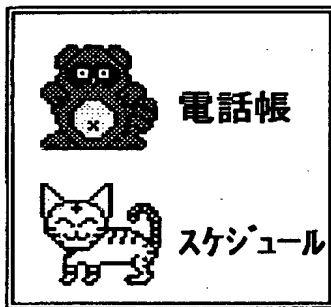


<https://www.hoge.com/foo2.gif>

802

【図 9】

901



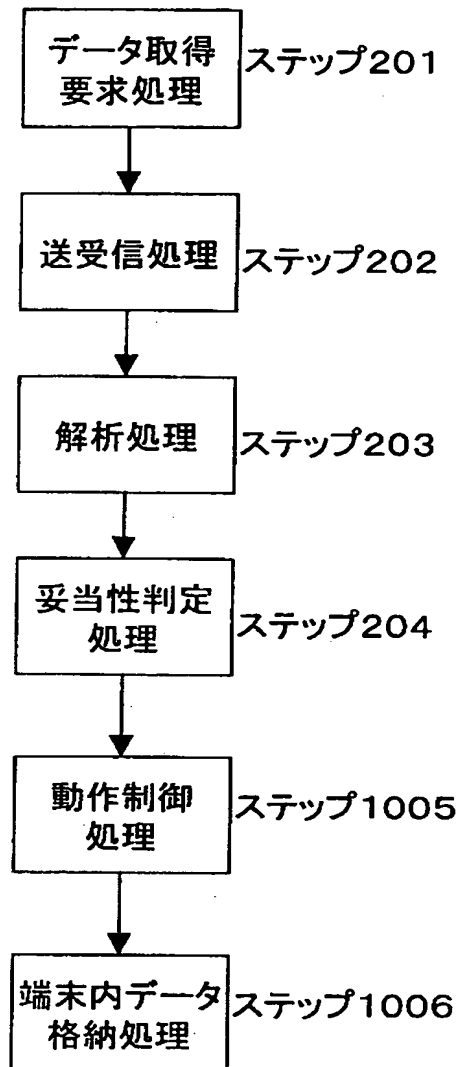
動作前

902

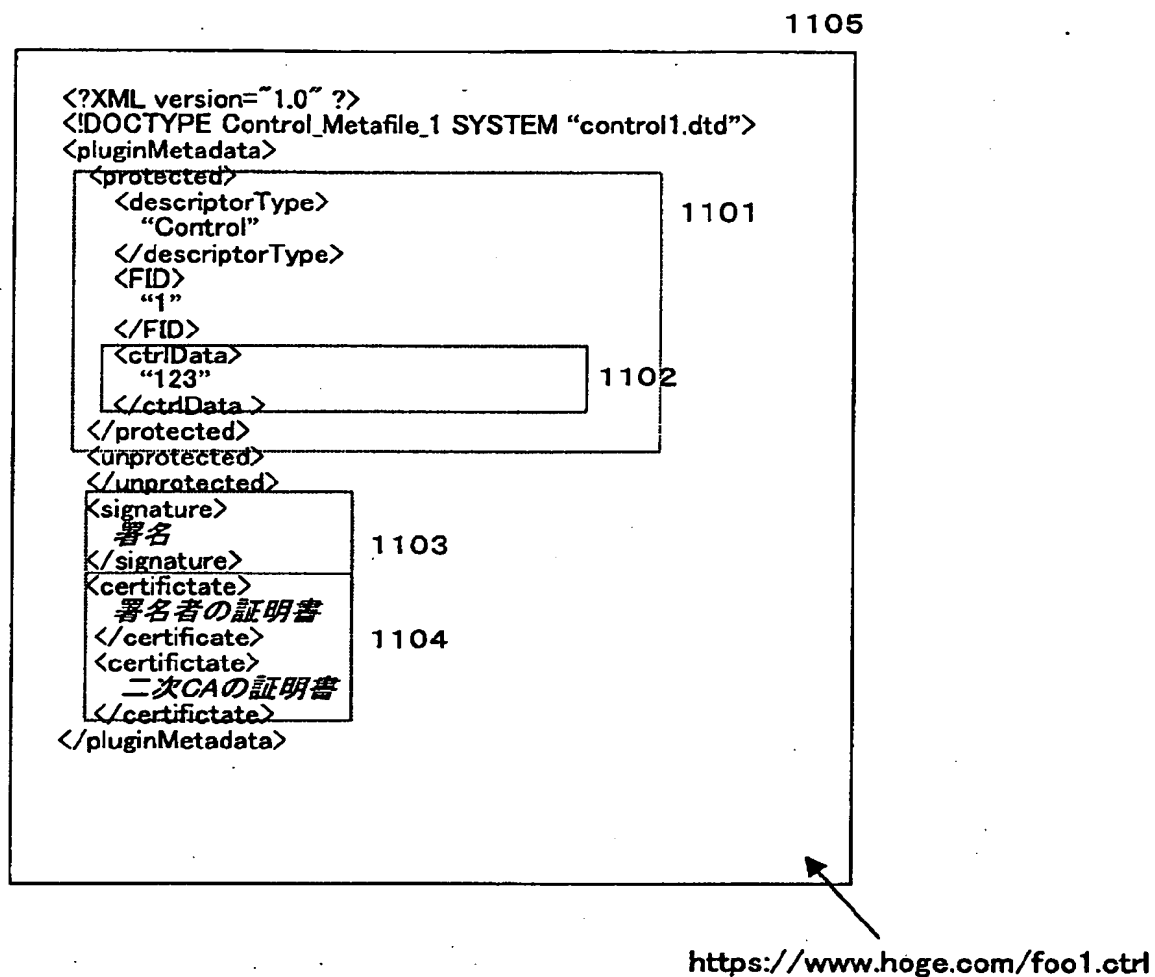


動作後

【図 1 0】



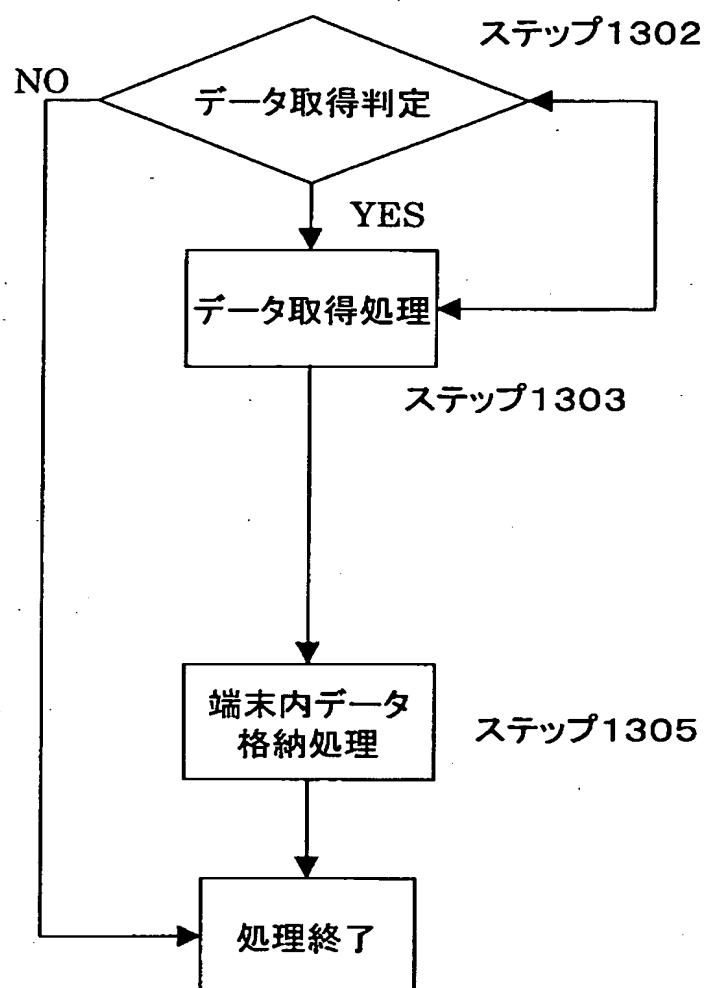
【図 11】



【図 12】

descriptorType	Control
FID	1
ctrlData	123
signature	署名
certificate	署名者の証明書
certificate	二次CAの証明書

【図13】



【書類名】 要約書

【要約】

【課題】 安全面を考慮すると J A V A アプレットといったプログラムから端末の周辺機器を制御することができなかった。

【解決手段】 J A V A アプレットのみに限らず、周辺機器へアクセスするプログラムにおいて、指示データに自身の妥当性を判定する方式を用いることによって、周辺機器の制御を安全に行える。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社